The patient, the logfile and the law

Herveg, Jean

Published in:
Droits des patients, mobilité et accès aux soins

Publication date:
2011

Document Version
Publisher's PDF, also known as Version of record

THE PATIENT, THE LOGFILE AND THE LAW [1]

Jean HERVEG *

I. – What is a log file ?

The log file, also called "log" or "trace file", is a computer file designed for recording predefined events or actions that may occur in a system or software. This definition calls for two clarifications. First, there is no automatic record of the actions or events that may occur in a system or software. Then, the log file records only the actions or events for which it was set. In other words, this file does not save everything that may happen in a system or software. It will only store the information it has been asked to record, no more no less.

Currently, we are interested in the log files of the patients' electronic records and the information they are likely to store, like the identity of the person who have accessed the record, the time of access, the accessed information, and the operations performed by the person when accessing the file (what document or information has been read, copied, modified, deleted, uploaded, transmitted to a third person, etc.?).

Satisfying the patients' requests to access the log files of their electronic health records requires to solve two questions: Is there any obligation to keep log files for their electronic health records? And do the patients have any right to access these log files?

Literally, Directive 95/46/EC does not specifically address the issue of log files. But it allows for considering the issue from two perspectives: that of the technical and organisational measures ensuring the security of the data processing, and that of the data subject's right of access.

---

[1] This paper is a shorter version of a paper published in 2010 in Lex Medicinae (Revista Portuguesa de Direito da Sùde).

* *Research Centre on IT and Law – Law School of Namur. Member of the Bar of Brussels.*

II. – Technical and organisational measures and log files

a. – Preventing unauthorized use of data

The European Court of Human Rights has repeatedly stressed the fundamental role of data protection for the right to respect for private and family life[2]. The Court held that the domestic legislation of the Contracting Parties to the Convention should afford appropriate safeguards to prevent any communication or disclosure of personal data concerning health that does not comply with the guarantees provided by Article 8 of the Convention[3]. Then, the Court extended this requirement to all personal data[4].

In the case of *S. & Marper v. United Kingdom*, the Court stated that, as regards personal data subject to automatic processing for police purposes, domestic law should in particular ensure that such information were relevant and not excessive in relation to the purposes for which they were recorded, and were kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which they were recorded. The Court stressed that the law should contain appropriate safeguards to effectively protect personal data against misuses and abuses. The Court further emphasized that these considerations matter even more when dealing with the protection of special categories of sensitive data, notably DNA data[5].

b. – One aspect of this prevention: organizational and technical measures to ensure data processing security

To ensure the protection of the data subject against the unauthorized use of personal data, Directive 95/46/EC requires the data controller to ensure that the data are processed fairly and lawfully, that their collection is made for specified, explicit and legitimate purposes and that they are not further

---

2 E.C.H.R., 25 February 1997, Z v. Finland, n° 22009/93, § 95; 27 August 1997, M.S. v. Sweden, n° 20837/92, § 41; 17 July 2008, I. v. Finland, n° 20511/03, § 38. See also: E.C.H.R., 25 November 2008, Biriuk v. Lithuania, n° 23373/03, §§ 39 & 43; 25 November 2008, Armonas v. Lithuania, n° 36919/02, §§ 40 et 44; 28 April 2009, K.H. & al. v. Slovakia, n° 32881/04, § 55; 6 October 2009, C.C. v. Spain, n° 1425/06, § 31.

3 Referring to, *mutatis mutandis*, articles 3 § 2.c, 5, 6 & 9 of the Convention of 28 January 1981 for the Protection of Individuals with regard to automatic processing of personal data, European Treaty Series, n° 108, Strasbourg, 1981; E.C.H.R., 25 February 1997, Z v. Finland, n° 22009/93, § 95; 27 August 1997, M.S. v. Sweden, n° 20837/92, § 41; 17 July 2008, I. v. Finland, n° 20511/03, § 38; 6 October 2009, C.C. v. Spain, n° 1425/06, § 32; 4 December 2008, S. & Marper v. United Kingdom, n° 30562/04 & 30566/04, § 103.

4 E.C.H.R., 4 December 2008, S. & Marper v. United Kingdom, n° 30562/04 & 30566/04, § 103.

5 E.C.H.R., 4 December 2008, S. & Marper v. United Kingdom, n° 30562/04 & 30566/04, § 103.

processed in a incompatible manner, that they are adequate, relevant and not excessive in relation to the purposes for which they are collected and processed, and also that they are kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which they were obtained and processed[6]. The Directive 95/46/EC provides the data subject with a right to get information on the data processing, rights of access and correction, and a right of objection and a right to receive compensation from the data controller in case of damages resulting of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to the Directive[7].

In addition to the notification of the data processing to the national supervisory authority[8], Directive 95/46/EC also requires that any person acting under the authority of the data controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the data controller, unless this person is required to do so by law[9].

In order to ensure the security of the data processing, the data controller « (...) *must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing* » provided that « *such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected, having regard to the state of the art and the cost of their implementation* »[10].

c. – *What about log files?*

Apparently, Directive 95/46/EC only imposes ***preventive*** security measures to ensure the protection of the data subjects when processing their personal data. This would mean that the data controller would not be required to take

---

6 Directive 95/46/EC, article 6.

7 Directive 95/46/EC, articles 10 – 15.

8 Directive 95/46/EC, articles 18 – 20.

9 Directive 95/46/EC, article 16.

10 Directive 95/46/EC, article 17. Cf. recital n° 46.
Article 4.1 bis of the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) provides that the technical and organizational measures aiming at safeguarding the security of the services offered by a provider of electronic communications service accessible to the public must at least ensure the implementation of a security policy with respect to data processing.

a posteriori measures, such as, for example, auditing measures. In other words, preventing unauthorized use of personal data would impose access policies but not log files, the latter being a kind of auditing measure, that is to say an *a posteriori* security measure. This interpretation, although it may rely on arguments based on a (too) literal interpretation of the text, can not be upheld. Indeed, it can not be seriously disputed that log files are a major security measure when processing personal data, at least owing to their deterrent effect against potential violators, which is only possible with an efficient identification system.

But the fact that log files are part of the range of technical and organizational measures that can ensure the security of data processing does not imply that any system or software that falls under the scope of Directive 95/46/EC should have log files. Indeed, their implementation is not automatic[11].

Thus, the answer to the question of whether log files should be implemented when processing personal data depends on a case by case analysis using these criteria[12]. In this respect, it is worth remembering that the greater the risk created by a data processing to the data subject, whether by the purpose of the data processing or the informational content of the data, the greater the need to prevent and punish the unauthorized processing of personal data. Similarly, the determination of actions or events to be recorded shall depend on the intensity of need to deter unauthorized data processing and make effective their repression.

One must well understand that the implementation of log files is likely to favourably influence the analysis of the legitimacy of the data processing, as its absence could produce the opposite effect.

As regards the protection of medical data, the Committee of Ministers of the Council of Europe recommends that the appropriate technical and organizational measures guarantee that we can verify and check who had access to the information system and which data have been introduced, when and by whom[13].

---

[11] Cf. also the Explanatory report on the Convention of 28 January 1981 for the Protection of Individuals with regard to automatic processing of personal data, n° 108, recital 49.

[12] On contrary, Regulation (EC) 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, expressly provides that it must be kept a record of which personal data have been communicated, at what times and to whom, that it must subsequently be possible to check which personal data have been processed, at what times and by whom (art. 22.2, f & g).

[13] Appendix to the Recommendation No. R (97) 5 on the Protection of Medical Data, Adopted on February, 13, 1997, point 9.2. See also point 11.2 of the Appendix to the Recommeandation Rec (2002) 9 on the protection of personal data collected and processed for insurance purposes, Adopted on September, 18 2002.

In its working document on electronic medical records, the Article 29 Data Protection Working Party indicates that the legal framework for security measures should include, in particular, the necessity of « *comprehensive logging and documentation of all processing steps which have taken place within the system, especially access requests for reading or for writing, combined with regular internal checks and follow-up on correct authorization* »[14].

The case of *I. v. Finland*[15] relates to a nurse who had seen his work contract not renewed after rumors have circulated about her health. The nurse had failed to obtain compensation before the Finnish courts who considered that she did not bring evidence of unauthorized access to her medical records which was kept in the hospital where she worked. Before the European Court of Human Right, she complained about the hospital's failure to ensure the safety of her medical data against unauthorized access or, within the meaning of the Convention, a breach of Finland's positive obligation to guarantee respect for her private life by a system of rules of data protection.

The Court noted that under Finnish law, the data controller must ensure that personal data are adequately protected against unauthorized access and that only the staff in charge of the patient could access the medical file. The Court also noted that it was undisputed that the purpose of these statutory provisions was to protect personal data against the risk of unauthorized access. It recalled in this connection that the need for adequate safeguards was particularly important when processing highly intimate and sensitive data, where, furthermore, the data subject worked at the hospital where she was treated. But here, the system of medical records did not allow for knowing the use that had been made of the patient's record as it only mentions the five most recent consultations and that information itself was erased when the file get back to the archives. For this reason, it was not possible to know whether there was or not any unauthorized access to the nurse's medical record. The Court noted, for its part, that it was not disputed that, at that time, the system that prevailed at the hospital also allowed staff members to read medical records even when they were not directly involved in the provision of care to the person.

Insofar as the applicant lost her case for compensation because she did not prove the causal relationship between the deficiencies in the rules applicable to the access to her medical data and the disclosure of information concerning her medical condition, the Court held that to put such a burden on the applicant neglected the fact that the faults in storing the medical record by the hospital were recognized. The Court stressed that it was obvious that if the

---

[14] Article 29 Data Protection Working Party, Working Document on the processing of personal data relating to health in electronic health records (EHR), 15 February 2007, WP 131, p. 20.

[15] E.C.H.R., 17 July 2008, I. v. Finland, n° 20511/03.

hospital had better protected medical records by restricting their access to healthcare professionals directly involved in the treatment of the applicant or by keeping a record of all persons who had access to the applicant's medical records, the latter would have been in a less unfavourable position before the domestic courts. For the Court, what was decisive is that the hospital's system of medical records was clearly not in compliance with the legal requirements applicable to it, something to which national courts did not granted the importance it should have received in its opinion.

The Court further noted that the Finnish Government did not explain why the guarantees offered by its national law had not been respected in the hospital. It also noted that it was only after the applicant's complaint that a retrospective review of data access was set up at the hospital[16].

The Court stated that the possibility of obtaining compensation for damages caused by an unauthorized disclosure of personal data was not a sufficient mean to protect the right to respect for private life. What was needed first was a real and effective protection excluding any possibility of unauthorized access.

It appears from the foregoing that log files constitute a mandatory security measure for electronic health records and they should register actions and events allowing at least to know who supplied or amended what information, who accessed what information and when, and what did the person with the information, even in the case of an isolated private practice.

d. – What is the status of the person whose actions are registered by the log files?

Unless removing much of their usefulness, log files require to identify users and track their actions in the system or software. It is therefore a processing of personal data having to comply with the requirements imposed by the national legislations transposing Directive 95/46/EC. The person whose actions are recorded by the log files has, therefore, the quality of data subject. The data subject has a right to be informed of the existence of this recording and a right of access these data. This processing of personal data will only be legitimate to the extent that the security measure in itself is justified.

[16] E.C.H.R., 17 July 2008, I. v. Finland, n° 20511/03, § 45.

e. – What should be done with the log files?

It is not enough to know that the log files are a mandatory security measure for electronic health records. The logfiles must be audited in order to detect any unauthorized operation[17].

III. – Data subject's right of access and log files

Without constraint at reasonable intervals and without excessive delay or expense, the data subject has the right to obtain from the data controller:

- confirmation as to whether or not data relating to oneself are being processed;
- information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed;
- communication in an intelligible form of the data undergoing processing and of any available information as to their source;
- knowledge of the logic involved in any automatic processing of data at least in the case of automated decisions[18].

As appropriate, the data subject has the right to obtain from the data controller the rectification, erasure or blocking of data the processing of which does not comply with the Directive, in particular because of the incomplete or inaccurate nature of the data, the notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out, unless this proves impossible or involves a disproportionate effort[19].

A first glance, none of this can justify any patients' right to access the log files of their electronic health records. Fortunately, the Court of Justice of the European Union has provided some clarification on this issue in a ruling dated May 7, 2009[20]. In this case, Mr. Rijkeboer asked the College of Rotterdam to inform him if information about him and from the municipal administration had been disclosed to third parties during the two years preceding his request. He wanted to know who these people were and the content of the information

---

17 Article 29 Data Protection Working Party agrees: « Regular internal and external data protection auditing of access protocols must take place (…) » (Working Document on the processing of personal data relating to health in electronic health records (EHR), 15 February 2007, WP 131, p. 21).

18 Directive 95/46/EC, article 12.

19 Directive 95/46/EC, article 12.

20 C.J.E.U., 7 May 2009, C-553/07, College van burgemeester en wethouders van Rotterdam v. M. E.E. Rijkeboer.

that had been transmitted to them. He had moved to another municipality and wanted to know, in particular, to whom his old address had been provided. He got an answer for the year preceding his request, previous data having been automatically deleted in accordance with the law of the Netherlands relating to personal data held by local authorities. The European Court of Justice was asked whether the right of access of the data subject to information about the recipients or categories of recipients of personal data as well as on the content of the data provided could be limited to a one-year period preceding the request for access.

The Court of Justice first noted that the right of access should, in particular, allow the data subjects to ensure the accuracy of their personal data as well as the legality of their processing. It also recalled that the data subjects should have a judicial remedy for violations of their rights and that the data controller owed compensation for damage suffered as a result of an unlawful processing or any act incompatible with the national rules on data processing.

The Court of Justice then observed that the obligation to retain data in a form which permits identification of the data subject for a period not exceeding that necessary to achieve the objective pursued by the data processing, and the right of access and the right to information about the recipients or categories of recipients, were intended to protect the data subject. The Court noted that the national jurisdiction wanted to know whether there was a link between these two elements, in the sense that the right of access to information about the recipients or categories of recipients of personal data and on the content of transmitted data, may depend on the duration of data retention. For some, once the data are erased, the right of access should disappear as a consequence. For others, the right of access includes not only the present, but also the period before the access request, without, however, unanimity on the exact duration of this right of access, which is not specified by the Directive.

In order to resolve this issue, the Court of Justice suggested to determine what data were covered by the right of access and, next, to turn to the objective of the right of access. In its approach, the Court of Justice made a judicious distinction between on the one hand, basic (personal) data and, secondly, information on recipients or categories of recipient to whom those basic data are disclosed and on the content thereof. This second category of information relates to the processing of the basic data; they are "meta-data". The Court noted that the time-limit on the right of access to information on the recipient or recipients of personal data and on the content of the data disclosed concerned that second category of data.

The remaining question is then of the compliance of this time-limit to access such data in relation to the purpose of the right of access. In this respect, the Court recalls that the right of access is necessary to enable the data subjects to exercise their rights, that is to say, when the processing of their data does not

comply with the provisions of the Directive, the right to have the controller rectify, erase or block their data, or notify third parties to whom the data have been disclosed of that rectification, erasure or blocking, unless this proves impossible or involves a disproportionate effort. The Court also reminded that the right of access is necessary to enable the data subjects to exercise their right to object to the processing of their personal data and their right of action when suffering damages.

The Court of Justice held that in order to ensure the practical effect of these rights, the right of access must of necessity relate to the past. If that were not the case, the data subjects would not be in a position effectively to exercise their right to have data presumed unlawful or incorrect rectified, erased or blocked or to bring legal proceedings and obtain compensation for the damage suffered.

Therefore, the only remaining question is the scope of that right in the past. In this respect, the Court reminded that the setting of a time-limit with regard to the right to access to information on the recipients or categories of recipient of personal data and on the content of the data disclosed must allow data subjects to exercise their different rights and that the length of time the basic data are to be stored may constitute a useful parameter without, however, being decisive.

Besides the fact that the time-limit of the right of access should allow for the data subjects to exercise their various rights, one should also take into account applicable provisions of national law on time-limits for bringing an action, the more or less sensitive nature of the basic data, the length of time for which those data are to be stored and the number of recipients.

In the case of electronic health records, the duration of this right of access should match at least with the time-limits of the patients' rights and the information on the processing of (basic) personal data should enable the implementation of the patients' rights, that is to say, at the very least, to know who supplied or amended what information, who accessed what information and when, and what did the person with the information, even in the case of an isolated private practice. Designed in this way, the right of access to information on the processing of (basic) personal data would strengthen the legitimacy of the objective pursued by the data processing.

IV. – Spontaneous communication of the log files to the patient

Although it also concerns the recipients or categories of recipients, the right of information on the processing of personal data does not include any obligation on the part of the data controller to provide the patients with the log files of their electronic health records. Indeed, when the data are collected

from the data subject, this obligation must be completed no later than when the data are obtained. When the data are not collected from the data subject, this information must be realised upon the storing of the data or, if a disclosure to a third party is envisaged, no later than at the time of the first communication[21].

However, as suggested by the Article 29 Data Protection Working Party: « *In order to establish trust, a special routine for informing the data subject when and who accessed data in his EHR could be introduced. Furnishing the data subjects in regular intervals with a protocol listing the persons or institutions who accessed their file would reassure patients about their ability to know what is happening to their data in the EHR system* »[22]. It added that « (...) *The already mentioned annual access report sent to the data subjects would be an additional effective means for checking legality of use of EHR data* (...) »[23].

This measure would also contribute to strengthen the legitimacy of the objective pursued by the data processing.

Conclusions

It is now clearly established that log files must record information on the processing of (basic) medical data, such as information on the recipients or categories of recipients to whom the data are disclosed or information on the content of the (basic) medical data. This kind of security measure would coincide with the implementation of the patient's right of access, both reinforcing the legitimacy of the objective pursued by the data controller. The log files must help to know who supplied or amended what information (information on the content of the basic data and information on the origin of the basic data), who get access to what information and when, and what did the person with the information, even in the case of an isolated private practice. The communication of the log files to the patients at regular intervals will also contribute to base the legitimacy of the purpose pursued by the data controller. Finally, the data controller must ensure regular audits of the log files in the context of a comprehensive security policy and this, with an effective system of user identification and registration of their actions.

[21] Directive 95/46/EC, articles 10 and 11. Cf. C.J.E.U., 7 May 2009, C-553/07, o.c., Recitals n° 68-69.

[22] Article 29 Data Protection Working Party, o.c., WP 131, p. 24.

[23] Article 29 Data Protection Working Party, o.c., WP 131, p. 24.